INFORMATICA, 2010, Vol. 21, No. 2, 215–228

Security Analysis of Asymmetric Cipher Protocol Based on Matrix Decomposition Problem

Andrius RAULYNAITIS, Eligijus SAKALAUSKAS, Saulius JAPERTAS

Kaunas University of Technology, Institute of Defense Technologies,
Department of Applied Mathematics, Department of Telecommunications
Studentų 50, LT-51368 Kaunas, Lithuania
e-mail: andrius.raulynaitis@stud.ktu.lt, eligijus.sakalauskas@ktu.lt, saulius.japertas@ktu.lt

Received: October 2008; accepted: May 2010

Abstract. The asymmetric cipher protocol, based on decomposition problem in matrix semiring $\mathcal{M}$ over semiring of natural numbers $\mathcal{N}$ is presented. The security of presented cipher protocol is based on matrix decomposition problem (MDP), which is linked to the problem of solution of multivariate polynomial system of equations. Compromitation of proposed scheme relies on the solution of system of multivariate polynomial system of equations over the semiring of natural numbers $\mathcal{N}$. The security parameters are defined, security analysis and implementation is presented.

Keywords: asymmetric cipher, matrix decomposition problem, one-way function.

1. Introduction

In recent years the public key cryptosystems are spreading into some application areas such as smart cards and e-commerce. There are some new results in the field of key exchange protocols and authentication schemes (Liu and Huang, 2010; Yoon and Yoo, 2009; Tseng, 2008). But nevertheless the asymmetric ciphers implementation in such a memory and computational power restricted devices seems to be also perspective. Except the smart cards the other examples of public key cryptosystems application can be considered. Among them are the mobile phones for the secret mobile communications. It is desirable to avoid the arithmetical operations with large integers in such a computational power restricted devices since they require a special co-processors.

In this paper we consider just another approach to construct the asymmetric cipher avoiding the arithmetical operations with large integers.

The asymmetric cipher constructing must be based on certain one-way function. According to general definition, OWF is a function, when computing its value for any argument is easy, but its inversion is not, i.e., this problem is intractable. Hence the security of asymmetric cipher relies on the complexity of OWF inversion.

New ideas in public key cryptography using hard problems in infinite non-commutative groups and semigroups appeared in Sidelnikov *et al.* (1993). One realization of these ideas appeared in Ko *et al.* (2000), using the braid group as a platform. The security of

this cryptosystem was based on conjugator search problem. But according Shpilrain and Ushakov (2004) this approach is not sufficient and necessary to achieve proper security.

Lately the idea to use matrix group conjugacy problem together with matrix discrete logarithm problem for the one way function construction is presented in Sakalauskas *et al.* (2007).

We propose to construct new asymmetric cipher using decomposition (double coset) problem in matrix semiring $\mathcal{M}$ over the semiring $\mathcal{N}$ of natural numbers. We will make a conjecture supported by our analysis, that this decomposition problem is intractable and hence is a candidate to be as OWF.

In this paper we analyze security aspects of decomposition (double coset) problem in matrix semiring $\mathcal{M}$ over the semiring $\mathcal{N}$ of natural numbers.

The construction of asymmetric cipher protocol with a brief mathematical background is presented in Section 2.

Section 3 provides considerations on the security analysis and implementation issue.

The main conclusions about security analysis and implementation of proposed algorithms are outlined in Section 4.

2. Asymmetric Cipher Protocol

We consider an infinite multiplicative matrix semiring $\mathcal{M}$ over the semiring of natural numbers $\mathcal{N} = \{0, 1, 2, \ldots\}$. The elements of $\mathcal{M}$ are m-dimensional square matrices with entries in $\mathcal{N}$. Let $\mathcal{P} = \{p_i()\}$ is a set of all polynomials over $\mathcal{N}$. Then the subset $\mathcal{M}_L \subset \mathcal{M}$ we define as a set of all matrices of all polynomial functions in $\mathcal{P}$ with argument $M_L \in \mathcal{M}_L$ and $\mathcal{M}_R \subset \mathcal{M}$ as a set of all polynomials functions with arguments $M_R \in \mathcal{M}_R$. In other words $\mathcal{M}_R$ and $\mathcal{M}_L$ are generated by M_L and M_R respectively, using polynomials functions from $\mathcal{P}$.

Hence for some non-commutating matrices M_L and M_R in $\mathcal{M}$ we can construct two subsets $\mathcal{M}_L$ and $\mathcal{M}_R$ of mutually commutating matrices respectively. Implicitly these sets can be defined as $\mathcal{M}_L = \{p_i(M_L) \mid p_i() \in \mathcal{P}\}$ and $\mathcal{M}_R = \{p_j(M_R) | p_j() \in \mathcal{P}\}$.

Two pairs of mutual commuting matrices M_{L1}, M_{L2} and M_{R1}, M_{R2} must be randomly generated in block diagonal form as follows:

$$M_{L1} = \begin{pmatrix} L_1 & \Theta \\ \Theta & l_1 I \end{pmatrix}, \qquad M_{L2} = \begin{pmatrix} l_2 I & \Theta \\ \Theta & L_2 \end{pmatrix},$$

$$M_{R1} = \begin{pmatrix} R_1 & \Theta \\ \Theta & r_1 I \end{pmatrix}, \qquad M_{R2} = \begin{pmatrix} r_2 I & \Theta \\ \Theta & R_2 \end{pmatrix}. \tag{1}$$

All block matrices $\Theta, L_1, L_2, R_1, R_2$ and I are square matrices of dimension $m/2$. Scalars $l_1, l_2 r_1$ and r_2 are in $\mathcal{N}$ and are chosen at random. A Θ is matrix with all zero elements, I is identity matrix with all zero elements except the main diagonal consisting of unit elements. Matrices L_1, L_2, R_1 and R_2 are chosen at random with elements in $\mathcal{N}$.

To avoid arithmetic with big integers, the elements of these matrices should be bounded, e.g., their values does not exceed some number $r \in \mathcal{N}$, e.g., $r = 9$.

According to this special construction in (1) we have that two pairs of block diagonal matrices M_{L1}, M_{L2} and M_{R1}, M_{R2} are mutually commuting due to its block diagonal structure.

$$M_{L1}M_{L2} = M_{L2}M_{L1}; \qquad M_{R1}M_{R2} = M_{R2}M_{R1}. \tag{2}$$

These identities could be easily verified. Mutually commuting are also matrices M_{L1}, M_{R2} and M_{L2}, M_{R1}, but this property is not used in our construction.

For example, randomly generated 4th order ($m = 4$) matrices in (1) with $r = 4$ could be of the following form:

$$M_{L1} = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 3 & 4 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 2 \end{pmatrix}, \qquad M_{L2} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 4 & 2 \\ 0 & 0 & 4 & 3 \end{pmatrix},$$

$$M_{R1} = \begin{pmatrix} 2 & 1 & 0 & 0 \\ 2 & 4 & 0 & 0 \\ 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 3 \end{pmatrix}, \qquad M_{R2} = \begin{pmatrix} 4 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 \\ 0 & 0 & 3 & 2 \\ 0 & 0 & 3 & 1 \end{pmatrix}.$$

Using randomly generated matrices M_{L1}, M_{L2} and M_{R1}, M_{R2} of the form (1), the following polynomial matrices can be calculated:

$$X = p_{X1}(M_{L1}) \cdot p_{X2}(M_{L2}), \tag{3}$$
$$Y = p_{Y1}(M_{R1}) \cdot p_{Y2}(M_{R2}), \tag{4}$$
$$U = p_{U1}(M_{L1}) \cdot p_{U2}(M_{L2}), \tag{5}$$
$$V = p_{V1}(M_{R1}) \cdot p_{V2}(M_{R2}). \tag{6}$$

where, as mentioned above, all polynomials are in $\mathcal{P}$. All coefficients $a_1 = (a_{10}, a_{11}, \ldots, a_{1n})$, $a_2 = (a_{20}, a_{21}, \ldots, a_{2n})$, $b_1 = (b_{10}, b_{11}, \ldots, b_{1n})$, $b_2 = (b_{20}, b_{21}, \ldots, b_{2n})$, $c_1 = (c_{10}, c_{11}, \ldots, c_{1n})$, $c_2 = (c_{20}, c_{21}, \ldots, c_{2n})$, $d_1 = (d_{10}, d_{11}, \ldots, d_{1n})$, $d_2 = (d_{20}, d_{21}, \ldots, d_{2n})$ of polynomials $p_{X1}, p_{X2}, p_{Y1}, p_{Y2}, p_{U1}, p_{U2}, p_{V1}, p_{V2}$ are generated at random in $\mathcal{N}$. For generation process their values should be bounded, i.e., their values do not exceed some number $s \in \mathcal{N}$.

It can be easily verified, that matrices X, U and Y, V are commuting: $XU = UX$, and $YV = VY$. Since due to special form of matrices M_{L1}, M_{L2} and M_{R1}, M_{R2}, the following identities takes place

$$\begin{aligned} XU &= p_{X1}\big(M_{L1}\big) \cdot p_{X2}\big(M_{L2}\big) \cdot p_{U1}\big(M_{L1}\big) \cdot p_{U2}\big(M_{L2}\big) \\ &= \sum_{i=0}^{n} a_{1i} M_{L1}^{i} \cdot \sum_{j=0}^{n} a_{2j} M_{L2}^{j} \cdot \sum_{k=0}^{n} c_{1k} M_{L1}^{k} \cdot \sum_{l=0}^{n} c_{2l} M_{L2}^{l} \end{aligned}$$

$$
\begin{aligned}
&= \sum_{i,j,k,l=0}^{n} \left(\overbrace{a_{1i}M_{L1}^{i} \cdot a_{2j}M_{L2}^{j}}^{X} \cdot \overbrace{c_{1k}M_{L1}^{k} \cdot c_{2l}M_{L2}^{l}}^{U} \right) \\
&= \sum_{i,j,k,l=0}^{n} \left(\overbrace{c_{1k}M_{L1}^{k} \cdot c_{2l}M_{L2}^{l}}^{U} \cdot \overbrace{a_{1i}M_{L1}^{i} \cdot a_{2j}M_{L2}^{j}}^{X} \right) \\
&= \sum_{k=0}^{n} c_{1k}M_{L1}^{k} \cdot \sum_{l=0}^{n} c_{2l}M_{L2}^{l} \cdot \sum_{i=0}^{n} a_{1i}M_{L1}^{i} \cdot \sum_{j=0}^{n} a_{2j}M_{L2}^{j} \\
&= p_{U1}\big(M_{L1}\big) \cdot p_{U2}\big(M_{L2}\big) \cdot p_{X1}\big(M_{L1}\big) \cdot p_{X2}\big(M_{L2}\big) = UX.
\end{aligned}
$$

For the protocol construction we choose any fulfilled square m-dimensional matrix Q in $\mathcal{M}$. We choose also at random secret vectors of polynomials' coefficients and calculate matrices $X \in M_L$ and $Y \in M_R$ by formulas (3), (4). Then compute matrix:

$$A = XQY. \tag{7}$$

The asymmetric cipher public parameters we declare: sets $\mathcal{M}$ and $\mathcal{P}$, and matrices $M_{L1}, M_{L2}, M_{R1}, M_{R2}$. For the public key (PuK) we can define the matrices A and Q and for the private key (PrK) consist matrices X and Y. In brief these keys we denote by $\mathrm{PuK} = \{A, Q\}$ and $\mathrm{PrK} = \{X, Y\}$ correspondingly.

By introducing matrices M_{L1}, M_{L2}, M_{R1} and M_{R2} in such a special way, we achieve not only the required commutation condition but we can also reduce the length of private key (PrK). Instead of storage matrices X and Y, represented by its elements, it is enough to store the coefficients of polynomials $p_{X1}, p_{X2}, p_{Y1}, p_{Y2}$. Then for the ciphering procedure matrices X and Y must be computed using (3) and (4). This has some sense since PrK must be carefully stored in some memory restricted electronic device. Then instead of storing matrices X, Y with $2m^2$ its elements in $\mathcal{N}$, we can store the only 4 $(n+1)$ numbers in $\mathcal{N}$, representing the coefficients of polynomials $p_{X1}, p_{X2}, p_{Y1}, p_{Y2}$.

The recommended secure key lengths are presented below in Section 3.

We present below the estimated number of operation to compute the matrix A. Let the multiplication of two matrices can be performed by the $O(m^3)$ time algorithm, where m is a matrix order. According to (3), (4) and (7) for the computation of matrix A it is required to compute matrix X and Y. Since they are the polynomial functions of matrices $M_{L1}, M_{L2}, M_{R1}, M_{R2}$ then assuming that the order of polynomials is n the asymptotic time of computing both X and Y is $O(nm^3/4)$.

Then computation of matrix A can be performed by the $O(nm^3/2)$ time algorithm.

EXAMPLE 1. For a generation PuK and PrK we choose an artificially small the following initial parameters: $m = 4$, $n = 2$, $s = 3$, $r = 3$. We generate at random the following matrices $M_{L1}, M_{L2}, M_{R1}, M_{R2}, Q$ and coefficient of polynomials

$a_1 = (a_{10}, a_{11}, a_{13}),\ a_2 = (a_{20}, a_{21}, a_{23}),\ b_1 = (b_{10}, b_{11}, b_{13}),\ b_2 = (b_{20}, b_{21}, b_{23})$:

$$M_{L1} = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 3 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \qquad M_{L2} = \begin{pmatrix} 3 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ 0 & 0 & 3 & 3 \\ 0 & 0 & 1 & 3 \end{pmatrix},$$

$$M_{R1} = \begin{pmatrix} 3 & 1 & 0 & 0 \\ 3 & 1 & 0 & 0 \\ 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 3 \end{pmatrix}, \qquad M_{R2} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 2 \\ 0 & 0 & 2 & 1 \end{pmatrix},$$

$$Q = \begin{pmatrix} 2 & 2 & 3 & 1 \\ 1 & 1 & 2 & 1 \\ 1 & 2 & 1 & 3 \\ 1 & 1 & 1 & 1 \end{pmatrix},$$

$$a_1 = \begin{pmatrix} 0 & 2 & 3 \end{pmatrix}, \qquad a_2 = \begin{pmatrix} 1 & 0 & 2 \end{pmatrix},$$
$$b_1 = \begin{pmatrix} 1 & 2 & 2 \end{pmatrix}, \qquad b_2 = \begin{pmatrix} 0 & 0 & 1 \end{pmatrix}$$

With generated variables we can compute X, Y by (3), (4) and then A by (7):

$$X = p_{X1}(M_{L1}) \cdot p_{X2}(M_{L2}) = \begin{pmatrix} 2090 & 1210 & 0 & 0 \\ 3630 & 2090 & 0 & 0 \\ 0 & 0 & 545 & 900 \\ 0 & 0 & 300 & 545 \end{pmatrix},$$

$$Y = p_{Y1}(M_{R1}) \cdot p_{Y2}(M_{R2}) = \begin{pmatrix} 121 & 40 & 0 & 0 \\ 120 & 41 & 0 & 0 \\ 0 & 0 & 949 & 1022 \\ 0 & 0 & 1022 & 949 \end{pmatrix},$$

$$A = XQY = \begin{pmatrix} 1613040 & 930600 & 289735 & 486445 \\ 1607320 & 927300 & 289190 & 485545 \\ 14718990 & 8487710 & 2234895 & 3882505 \\ 14718990 & 8640280 & 2278695 & 3962075 \end{pmatrix}.$$

With this toy example we are able to encrypt to encrypt more than 400 bits information since the matrix A is represented by 400 bits.

To describe the ciphering processes we need to introduce the definition of encryptor and decryptor operators, using two randomly chosen secret matrices $U \in \mathcal{M}_L$ and $V \in \mathcal{M}_R$. These matrices are calculated by formulas (5), (6) using polynomials with randomly chosen secret coefficients.

DEFINITION 1. Encryptor ε is an element in $\mathcal{M}$, which is calculated by following equation:

$$\varepsilon = UAV. \tag{8}$$

DEFINITION 2. Decryptor δ is an element in $\mathcal{M}$, which is calculated by following equation:

$$\delta = UQV. \tag{9}$$

Since the finite elements of $\mathcal{N}$ can be transformed to the binary form, we define the bitwise XOR operation in $\mathcal{N}$ for any finitely presented numbers.

DEFINITION 3. The bitwise XOR operation $\oplus$ of numbers in $\mathcal{N}$ is a sum modulo 2 of bits of these numbers presented in binary form.

Let Alice wants to send Bob a message t, encrypted by asymmetric cipher. For encryption Alice uses Bob's public key $\mathrm{PuK} = \{A, Q\}$. The decryption is provided by the Bob's private key $\mathrm{PrK} = \{X, Y\}$.

At first, to encrypt a message t Alice must perform an encoding t by the set of finite numbers in $\mathcal{N}$ and to form a m-dimension encoded matrix T, corresponding to t.

The asymmetric cipher encryption algorithm is the following:

Step 1: Alice takes $M_{L1}, M_{L2}, M_{R1}, M_{R2}$ matrices, chooses four polynomials in $\mathcal{P}$ with secret random generated coefficients and using (5), (6) calculates matrices U and V.

Step 2: Alice takes Bob's PuK and using (8) calculates encryptor ε.

Step 3: Alice calculates decryptor δ using (9) in a similar way.

Step 4: Alice obtains the cyphertext C computed by the formula:

$$C = \varepsilon \oplus T = UAV \oplus T. \tag{10}$$

Step 5: Alice sends to Bob the following data $D = (C, \delta)$.

Decryption algorithm:

Bob gets data $D = (C, \delta)$ and using his private key $\mathrm{PrK} = \{X, Y\}$ calculates the encoded plaintext T by equations:

$$X\delta Y \oplus C = T. \tag{11}$$

The last equation is valid since the following identities holds

$$XU = UX \quad \text{and} \quad VY = YV,$$

and

$$\begin{aligned} X\delta Y \oplus C &= X\,(UQV)\,Y \oplus C = X\,(UQV)\,Y \oplus UAV \oplus T \\ &= XUQVY \oplus UXQYV \oplus T = UXQYV \oplus UXQYV \oplus T = T. \end{aligned}$$

Then Bob, using the known decoding procedure recovers the initial message t from T.

3. Security Analysis and Implementation

The full system of equation available for the adversary to break the system is the following matrix equations:

$$\begin{cases} XQY = A, \\ UQV = \delta, \\ UAV \oplus T = C. \end{cases}$$

Hence we have three matrix equations with five unknowns matrices X, Y, U, V and T. In scalar form, we have $3m^2$ bi-quadratic equations with unknown coefficients $(a_{10}, a_{11}, \ldots, a_{1n})$, $(a_{20}, a_{21}, \ldots, a_{2n})$, $(b_{10}, b_{11}, \ldots, b_{1n})$, $(b_{20}, b_{21}, \ldots, b_{2n})$, $(c_{10}, c_{11}, \ldots, c_{1n})$, $(c_{20}, c_{21}, \ldots, c_{2n})$, $(d_{10}, d_{11}, \ldots, d_{1n})$, $(d_{20}, d_{21}, \ldots, d_{2n})$, of polynomials $p_{X1}, p_{X2}, p_{Y1}, p_{Y2}, p_{U1}, p_{U2}, p_{V1}, p_{V2}$ and unknown elements of encoded matrix T. Hence by considering the above system of three matrix equations we have $8(n+1)$ unknown polynomials coefficients and m^2 encoded matrix T elements $\{t_{ij}\}$. In total we have $8(n+1) + m^2$ unknowns.

To solve this total system is too cumbersome and not required for the adversary since it has too large number of equations and unknowns. We can see that the first matrix equation is independent of other two equations and hence it can be considered independently. Let as consider the second and the third system of matrix equations.

To decrypt C he (she) must find the exact matrix T and hence any two matrices U' and V', related with T. If adversary tries to find an arbitrary matrix T' and corresponding arbitrary matrices U'', V'' this attack has no sense. If the adversary finds the exact matrix T and any two matrices U'', V'' this attack does not totally break the system but only decrypts the ciphertext C. Hence the solution of only second and third equations is cumbersome and they must be solved for every ciphertext C.

For the total breaking of the system it is enough to solve the only first matrix equation $XQY = A$ and to find *any* unknown matrices X' and Y'. This equation is independed from other two equations since it has different unknowns and hence can be treated independently of remaining other two matrix equations.

The adversary can concentrate his attempt to solve only this one matrix equation not only to decrypt the ciphertext C, i.e., to find encoded matrix T but also to break totally the system by finding other forged system's private key X' and Y'. This allows adversary to decrypt any ciphertext C.

Hence we concentrate our attempt to this simplified method of attack.

According Garey and Johnson (1979) the solution of multivariate algebraic equations in field is NP-complete problem. For further analysis we must define the matrix decomposition problem (MDP), which is linked to the problem of solution of multivariate algebraic equations. We will show that on the complexity of MDP relies the security of proposed cipher algorithm.

DEFINITION 4. The computational matrix decomposition (or double coset) problem (MDP) is to find any matrices X' and Y', when given matrices Q and A from the follow-

ing equation:

$$X'QY' = A. \tag{12}$$

In addition to this MDP formulation the extra conditions to the matrices X', Y' are introduced, i.e., the satisfiability of certain commutation conditions. For certain matrices U, V the matrices X' and Y' must satisfy the commutation identities $X'U = UX'$ and $Y'V = VY'$.

The solution of (12) without any restriction to the matrices X' and Y' over the field is trivial. Indeed if we choose any matrix $Y' = Y_0$ then we can find the suitable matrix X' by denoting $QY_0 = R$ and solving the following linear system of equations, written in matrix form:

$$X'R' = A. \tag{13}$$

We will consider the MDP problem, when (12) is defined over semiring $\mathcal{N}$ and compare it with the MDP problem defined over finite ring and finite field.

Notice, that in any case if the matrices $X' \in M_L$ and $Y' \in M_R$ could be found, the adversary can decrypt message, using the following identities:

$$\begin{aligned} X'\delta Y' \oplus C &= X'(UQV)Y' \oplus C = U(X'QY')V \oplus UAV \oplus T \\ &= UAV \oplus UAV \oplus T = T. \end{aligned} \tag{14}$$

DEFINITION 5. The decisional (YES/NO) MDP is to get an answer, if there are any matrices X' and Y' in $\mathcal{M}$ satisfying (11) for given Q and A.

DEFINITION 6. The MDP is strong one way function (OWF) if either determination of any X' is infeasible when given A, Q and Y' or determination of any Y' is infeasible when given A, Q and X'.

Security of cipher algorithm relies on the complexity of computational MDP. It can be considered as a problem to find any vectors $a'_1 = (a'_{10}, a'_{11}, \ldots, a'_{1n})$, $a'_2 = (a'_{20}, a'_{21}, \ldots, a'_{2n})$, $b'_1 = (b'_{11}, b'_{12}, \ldots, b'_{1n})$ and $b'_2 = (b'_{21}, b'_{22}, \ldots, b'_{2n})$ of coefficients of polynomials p_{X1}, p_{X2} and p_{Y1}, p_{Y2} to compute the matrices X' and Y'. In this case system (12) can be rewritten in the following way:

$$X'QY' = \sum_{i,j,k,l} (a'_{1i}a'_{2j}b'_{1k}b'_{2l}M^i_{L1}M^j_{L2}QM^k_{R1}M^l_{R2}). \tag{15}$$

This matrix equation corresponds to the $m \times m$ system of polynomial equations with fourth order unknown monomials denoted by $a'_{1i}a'_{2j}b'_{1k}b'_{2l}$. Hence there are m^2 equations and 4 $(n+1)$ unknowns in every equation. Depending on m^2 and $4(n+1)$ ratio, this system is:

a) under defined, when $m^2 < 4(n+1)$;

b) equal defined, when $m^2 = 4(n+1)$;
c) over defined, when $m^2 > 4(n+1)$.

The proposed cipher's algorithm depends on the following parameters:

– dimension m of matrices;
– maximum range r of matrices' $(M_{L1}, M_{L2}, M_{R1}, M_{R2}, Q)$ elements (the number of digits for matrices element representation);
– maximum order n of polynomials;
– maximum range s of polynomials' coefficients.

Hence security of proposed cipher algorithm is based the solution of system of multivariate equations of fourth order.

So far there is some known methods as Grobner bases, linearization, XL and XSL that are dealing with a problem of solution of multivariate polynomial system of equations (Courtois *et al.*, 2000; Courtois and Pieprzyk, 2002; Biryukov and Canniere, 2003; Cid and Leurent, 2005). They efficiency depends on the concrete system properties and hence these methods are mainly ad-hoc methods. Moreover, the problem of multivariate polynomial system solution over the semiring is much worse than in case of the field and the methods of solution are not known yet. In our cases we have a non-sparse system of multivariate polynomial equations and hence we do not know any ideas on how to effectively realize the methods listed above.

The one way to analyze the complexity of (12) system solution, we think is the estimation of number of possible solutions, i.e., to find the set $\{a_1, a_2, b_1, b_2\}$ of vectors satisfying (12) using mathematical modeling. It is infeasible to investigate this question in general, or the real working examples. So we performed our investigation in reduced system dimensions for under, equal and over defined system's cases:

a) for under define case ($m^2 < 4(n+1)$) modeling was performed with $m = 4$ and $n = 4$;
b) for equal define case ($m^2 = 4(n+1)$) modeling was performed with $m = 4$ and $n = 3$;
c) for over define case ($m^2 > 4(n+1)$) modeling was performed with $m = 4$ and $n = 2$.

To provide modeling experiment the certain values of parameters m, n, r, s should be chosen. They define under, equal or over defined cases. After that matrices $M_{L1}, M_{L2}, M_{R1}, M_{R2}$ must be generated in predefined form (1). To construct matrices X and Y the $n+1$ coefficients for each polynomial $p_{X1}, p_{X2}, p_{Y1}, p_{Y2}$ should be chosen at random. Using (3) and (4) we calculate matrices X and Y and by (7) formula we compute matrix A.

The number of possible solution X, Y of equation $XQY = A$ was investigated using total scan to find the set of other matrices X' and Y', satisfying the equation $X'QY' = A$, where X' and Y' are defined by the polynomial coefficients.

Surprisingly but the mathematic modeling for these low dimension systems has showed, that when considering the systems of equations over semiring $\mathcal{N}$ in every case it has only one true solution. The other mathematical model was carried out in the case, when systems of equations were over the ring $\mathcal{Z}_N$ and N was a composite number. In this

case considerable big set of solutions was found in under defined system. Hence there is no-negligible probability to guest the solution in this case.

The other question is to investigate the complexity of this system, from the point of view of complexity theory. The valuable tool is to use the Shafer's dichotomy theorem (Shaefer, 1978). Schaefer examined satisfiability of propositional formulas for certain syntactically restricted formula classes. Each such class is given by a set S of Boolean functions (logical relations) allowed when constructing formulas.

DEFINITION 7. S-formula is any conjunction (&) of relations $R_1 \& R_2 \ldots \& R_k$.

DEFINITION 8. The SAT(S) problem is the problem of deciding whether a given S-formula is satisfiable.

Schaefer proved Dixotomy theorem which characterizes the complexity of SAT(S) for every finite set S of logical relations. The most striking feature of this characterization is that for any such S, SAT(S) is either polynomial-time decidable or NP-Complete.

According to these considerations, only one sensible method to estimate the security of proposed scheme is to choose the algorithm parameters preventing brute force attack. This approach is reasonable since the solution of system of multivariate polynomial equation over the field in most cases is comparable with a total scan of solutions.

The distinguishing line between these two extreme classes is characterized by the following conditions defined below relations (Couceiro, 2003).

DEFINITION 9. The relation R_i is said to be:

(a) 0-*valid* if when zero (false) values $(0, \ldots, 0)$ are assigned to the vector $(y_1, \ldots, y_L)$ then $R_i = 1$;
(b) 1-*valid* if when unit (true) values $(1, \ldots, 1)$ are assigned to the vector $(y_1 \ldots, y_L)$ then $R_i = 1$;
(c) *Horn* if $R_i(y_1, \ldots, y_L)$ is logically equivalent to some CNF (Conjunctive normal form) formula having at most one unnegated variable in each conjunct;
(d) *co-Horn* if $R_i(y_1, \ldots, y_L)$ is logically equivalent to some CNF formula having at most one negated variable in each conjunct;
(e) *bijunctive* if $R_i(y_1, \ldots, y_L)$ is logically equivalent to some CNF formula having at most 2 literals in any conjunct;
(f) *affine* if $R_i(y_1, \ldots, y_L)$ is logically equivalent to some system of linear equations over two-element field $\mathrm{Z}_2 = \{0, 1\}$.

There are corresponding criteria to check whether any relation R_i in S satisfies the properties (c)–(f) (Shaefer, 1978; Courtois and Pieprzyk, 2002; Biryukov and Canniere, 2003). The relation R_i is said to be:

(c') *Horn*, iff for all vectors $x, y \in R_i$ the vector $x \& y$ (obtained by, component-wise conjunction) is also in R_i;
(d') *co-Horn*, iff for all vectors $x, y \in R_i$ the vector $x \cap y$ (obtained by, component-wise disjunction) is also in R_i;

(e') *bijunctive*, iff for all vectors $x, y, z \in R_i$ the vector maj(x, y, z) (obtained by, component-wise majority) is also in $\in R_i$;

(f') *affine*, iff for all vectors $x, y, z \in R_i$ the vector $x+y+z$ (obtained by, component-wise triple sum) is also in R_i;

The mathematic modeling was performed in the cases when the (12) system of equations was under, equal and over defined over ring $\mathcal{Z}_6$:

(a) for under define with parameters $m = 4$ and $n = 4$;
(b) for equal define with parameters $m = 4$ and $n = 3$;
(c) for over define with parameters $m = 4$ and $n = 2$.

For the verification of conditions (a)–(f) in this case the same set of parameters were used as above. The total scan was performed in the set of all possible polynomial $p_{X1}, p_{X2}, p_{Y1}, p_{Y2}$ coefficients. In this way the total set of X' and Y' matrices was scanned. The conditions (a)–(f) were verified for the matrices X' and Y' satisfying the equation $X'QY' = A$.

Practical verification of condition (a)–(f) was performed in similar way, as described above.

The results showed, that for this instance, no one condition (a)–(f) was satisfied. Intuitively we can make a conjecture, that for instances with a higher dimension matrices and larger fields $_N(N > 6)$ to satisfy the conditions (a)–(f) is even harder.

Since for a higher dimensions and $N > 6$ the total scan of $(y_1, \ldots, y_L)$ assignments is infeasible, mathematical modeling showed that there was not found the assignments $(y_1, \ldots, y_L)$ satisfying (a)–(f) by scanning billions of randomly choosing assignments. Hence proposed function can be a good candidate for a one-way function.

The one of possible attack to find any matrices X' and Y' in (12) is to simulate them by other matrices choosing from the set $\{N^i \cdot M^j; i, j \in 0 \ldots n\}$ in order to reduce number of variables to be searched.

Modeling results showed, that in this case there was found no any solution in the case, when system of equation was defined over $\mathcal{N}$. The main security parameters we choose the maximum order n of polynomials and maximum range s of polynomials' coefficients. The reasonable values for the security parameters for our construction we choose those ones that prevent the brute force attack since the known methods for the solution of multivariate polynomial system of equations are comparable with the total scan of the possible solutions set. The total scan to find unknown coefficients of the polynomials requires performing the number η of verification operations, which can be expressed as follows:

$$\eta = s^{4n+4}. \tag{16}$$

The greater values s, n are, the higher security against the brute force attack can be achieved, but at the same time they increase the volumes of the PrK and PuK lengths. Hence s and n can be treated as security parameters.

Let, for example, choose the values: $s \in [0, \ldots, 63]$ (6 bit representation); $r \in [0, \ldots, 3]$ (2 bit representation); $n = 3$; $m = 8$, then number of verification operations is $\eta = 2^{128}$. Since the private key PrK$= \{X, Y\}$ can be represented by the vectors

of polynomials coefficients, then |PrK| = 128 bits. The representation of PuK= $\{A, Q\}$ requires *4608 bits*. Hence the PrK compromitation by applying the brute force attack has 2^{128} complexity.

4. Conclusion

1. In this paper the new asymmetric cipher scheme based on the matrix decomposition (dual coset) problem over the semiring of natural numbers $\mathcal{N}$ is proposed.
2. According to preliminary investigations based on the Shafer's dichotomy theorem and mathematical modeling, we can make a conjecture that the security of proposed scheme relies on the complexity of generalized satisfiability problem, which is reckoned as NP-complete.
3. Moreover, the compromitation of proposed scheme relies on the solution of system of multivariate polynomial system of equations over the semiring of natural numbers $\mathcal{N}$. The degree of monomials of system of equations is four. It is known (Garey and Johnson, 1979) that even the solution of multivariate quadratic polynomial system of equation over any field is NP-complete problem.
4. The security parameters of proposed scheme are presented taking into account the 3rd conclusion and the fact that the problem of multivariate polynomial system solution over the semiring is much more worse than in case of the field and the methods of solution are not known yet. Therefore we propose the security parameters preventing brute force attack.

References

Biryukov, A., Canniere, C. (2003). Block cipher and systems of quadratic equations. In: *Proceedings of FSE'2003, LNCS*, Vol. 2887, pp. 274–289.

Cid, C., Leurent, G. (2005). An analysis of the XSL algorithm. *ASIACRYPT 2005, LNCS*, Vol. 3788, pp. 333–335.

Couceiro, M. (2003). The complexity of constraint satisfaction: Shaefer's dichotomy theorem via post's clasification. Available at: `http://mtl.uta.fi/Opetus/seminaarit/AMTS/0304/CSP_miguel.ps`.

Courtois, N.T., Klimov, A., Patarin, J., Shamir, A. (2000). Efficient algorithms for solving overdefined systems of multivariate polynomial equations. In: *Eurocrypt'2000, LNCS*, Vol. 1807, Springer-Verlag, pp. 392–407.

Courtois, N.T., Pieprzyk, J. (2002). Cryptanalysis of block ciphers with overdefined systems of equations. In: *Proceedings of Asiacrypt'2002, LNCS*, Vol. 2501, Springer-Verlag, pp. 267–287.

Garey, M., Johnson, D. (1979). *Computers and Intractability: A Guide to Theory of NP-Completeness*. Freeman, New York.

Ko, K.H., Lee, S.J., Cheon, J.H., Han, J.W., Kang, J.–S., Park, C. (2000). New public–key cryptosystem using braid groups. In: *Advances in Cryptology, Proc. Crypto 2000, LNCS*, Vol. 1880, Springer–Verlag, pp. 166–183.

Liu, J., Huang, S. (2010). Identity-based threshold proxy signature from bilinear pairings. *Informatica*, 21(1), 41–56.

Sidelnikov, V., Cherepnev, M., Yaschenko, V. (1993). Systems of open distribution of keys on the basis of noncommutative semigroups. *Rus. Acad. Sci. Dokl. Math.*, 48(2), 566–567.

Sakalauskas, E., Tvarijonas, P., Raulynaitis, A. (2007). Key agreement protocol (KAP) using conjugacy and discrete logarithm problems in group representation level. *Informatica*, 18(1), 115–124.

Shaefer, T.J. (1978). The complexity of satisfiability problems. In: *Proc. of the 10th Annual Symposium on Theory and Computing*, pp. 216-226.

Shpilrain, V., Ushakov, A. (2004). The conjugacy search problem in public key cryptography: unnecessary and insufficient. Available at: `http://eprint.iacr.org/2004/321`.

Tseng, Y.-M., Wu, T.-Y., Wu, J.-D. (2008). A pairing-based user authentication scheme for wireless clients with smart cards. *Informatica*, 19(2), 285–302.

Yoon, E.-J., Yoo, K.-Y. (2009). Robust key exchange protocol between set-top box and smart card in DTV broadcasting. *Informatica*, 20(1), 139–150.

A. Raulynaitis – PhD student in Institute of Defense Technologies of Kaunas University of Technology. His current research interests are cryptography and asymmetric ciphering algorithms.

E. Sakalauskas – professor in Department of Applied Mathematics, Kaunas University of Technology. He received PhD degree from Kaunas University of Technology in 1983. The scope of scientific interests is a system theory, identification and cryptography. In these fields there were published about 50 papers. In recent time his research interest is focused mainly in the cryptography. There were obtained some results in the following fields: one way function construction based on the hard problems in infinite non-commutative groups representation level, digital signature schemes, key exchange protocols and pseudorandom number generation. The obtained recent research results in cryptography were published in about 10 papers.

S. Japertas received PhD in 1991. He is an associated proffesor of Telecommunications Department in Kaunas University of Technologies. Main research interests are wireless communications networks and systems; telecommunications and information security, safety and protection.

Asimetrinio šifravimo algoritmo, paremto matricos dekompozicijos problema, saugumo analizė

Andrius RAULYNAITIS, Eligijus SAKALAUSKAS, Saulius JAPERTAS

Šiame straipsnyje yra pasiūlytas asimetrinio šifravimo algoritmas, paremtas matricos dekompozicijos problema. Asimetrinio šifravimo algoritmo saugumas paremtas matricos dekompozicijos algoritminiu uždaviniu, kuris susijęs su daugelio kintamųjų algebrinių lygčių uždavinio sprendimu natūraliųjų skaičių pusžiedyje. Taip pat yra pateikta saugumo analizė, apibrėžti saugumo parametrai.